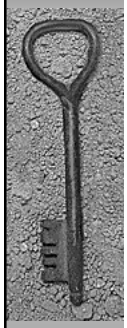
Key Management Guidelines

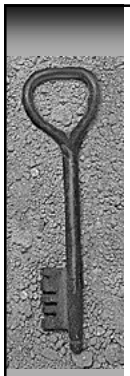
Introduction, Glossary, and Acronyms

Tim Polk, NIST



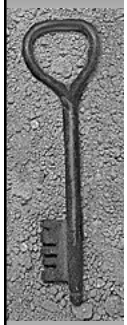
History

- Key Management Workshop #1 identified the need for a guidelines document as a companion to the Key Management Schemes document
  - Scope and audience were not defined



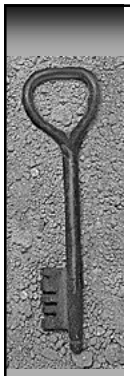
Scope

- Scope evolved over time
  - In principle, should be as narrow as possible
  - In practice, we need to fill out our current document suite
- New items still being added
  - Key confirmation
  - Selecting key derivation functions



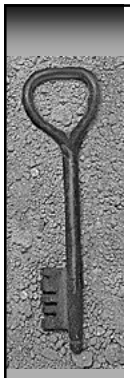
Scope, Cont'd

- In the end, our scope is everything that is:
  - outside the mathematics of the key management schemes; AND
  - not covered in current NIST documents



Audiences

- In principle, one focused audience is best
- In practice, NIST has numerous communities to serve and limited resources
- Three audiences targeted:
  - Standards developers
  - Implementers
  - System administrators



Protocol Developers

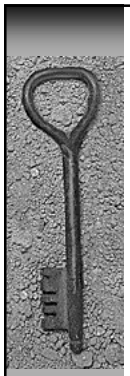
- Protocol developers need guidance and a toolkit of appropriate building blocks
  - The toolkit is the FIPS algorithms
  - This document must provide the guidance

Cryptographic Module Implementers

- Different applications impose different key management requirements
  - Module developers may gain greater understanding of the features required to support target applications

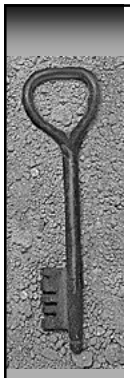
Systems Administrators

- A system is composed of products that were developed by third parties
- Configuration and selection of components is critical to the level security that is actually achieved
  - Cryptographic modules
  - Protocol stacks
  - Applications



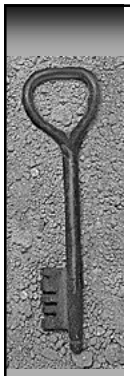
Consequences

- Document is a bit unwieldy
  - It includes information of marginal interest to every audience
- Document is very comprehensive



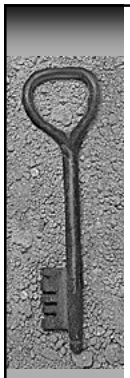
Overview

- Introduction
- Guidelines
- Algorithms, Keys, and Keying Material
- Key Management Lifecycle
- General Key Management Guidance
- Selected Infrastructures
- Selected Protocols
- Selected Applications



Algorithms, Keys, and Keying Material

- Classes of algorithms
- Classes of keys
- Protection requirements for different classes of keys

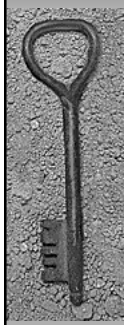


Key Management Lifecycle

- Framework for the lifecycle of a cryptographic key

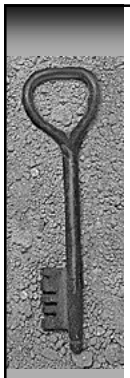
General Key Management Guidance

- Key management policy
  - Key usage, key lifetime, auditing, key recovery, etc.
- Cryptographic algorithm and key size selection
  - Assembling an appropriate suite of algorithms
- Key establishment schemes (placeholder)



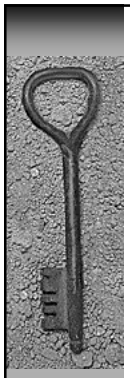
Selected Infrastructures

- Guidance on key management requirements for selected infrastructures
  - Expect to cover Kerberos and PKI



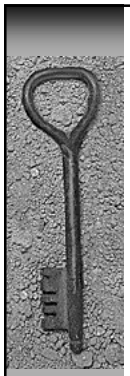
Selected Protocols

- Guidance on key management requirements for selected protocols (assumes multiple participants)
  - TLS
  - S/MIME
  - Others?



Selected Applications

- Guidance on key management requirements for selected applications
  - Assumption is one participant
  - Example is encrypted file storage



Glossary of Terms and Acronyms

- Eighty five terms defined
- Fourteen acronyms